

Congruent Elliptic Curves with Non-trivial Shafarevich-Tate Groups: Distribution Part

Zhangjie Wang

November 13, 2015

Abstract

We study the distribution of a subclass congruent elliptic curve $E^{(n)} : y^2 = x^3 - n^2x$, where n is congruent to 1 (mod 8) with all prime factors congruent to 1 (mod 4). We prove an independence of residue symbol property. Consequently we get the distribution of rank zero such $E^{(n)}$ with 2-primary part of Shafarevich-Tate group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. We also obtain a lower bound of the number of such $E^{(n)}$ with rank zero and 2-primary part of Shafarevich-Tate group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$.

1 Introduction and Main Theorem

A positive integer n is called a congruent number if it is the area of a right triangle with rational side lengths; or equivalently, the Mordell-Weil group of the elliptic curve $E^{(n)} : y^2 = x^3 - n^2x$ has positive rank. Let E be the elliptic curve over \mathbb{Q} defined by $y^2 = x^3 - x$, then $E^{(n)}$ is a quadratic twist of E . We are interested in the behavior of arithmetic groups such as Mordell-Weil groups and Shafarevich-Tate groups in the quadratic twist family of E .

Goldfeld conjectured that for any elliptic curve over \mathbb{Q} there are 50% elliptic curves with Mordell-Weil rank 0 and 1 respectively in its quadratic twist family. So far, this conjecture hasn't been verified for any single elliptic curve. The modular curve $X_0(19)$ has genus one and its cusp at ∞ is rational over \mathbb{Q} . For the elliptic curve $(X_0(19), [\infty])$, Vatsal [1] has proved that there are positive portion rank 0 elliptic curves in its quadratic twist family, and so is rank 1.

In this paper, we consider the distribution of congruent elliptic curves $E^{(n)}$ with Mordell-Weil rank 0 and non-trivial 2-primary Shafarevich-Tate groups. For a positive integer k , we denote Q_k to be the set of positive square-free integers n satisfying:

- $n \equiv 1 \pmod{8}$ with exactly k prime factors;
- any prime factor of n is congruent to 1 modulo 4.

Our main result in this paper is the following.

Theorem 1. *For any positive integer k , let $Q_k(x)$ be the set of integers $n \in Q_k$ with $n \leq x$, and $P_k(x)$ consist of those $n \in Q_k(x)$ satisfying*

$$\text{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0, \quad \text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

where $E^{(n)}(\mathbb{Q})$ is the Mordell-Weil group of $E^{(n)}$ and $\text{III}(E^{(n)}/\mathbb{Q})$ is the Shafarevich-Tate group of $E^{(n)}$. Then

$$\lim_{x \rightarrow \infty} \frac{\#P_k(x)}{\#Q_k(x)} = \frac{1}{2} \left(u_k + (2^{-1} - 2^{-k})u_{k-1} \right)$$

where $u_k := \prod_{i=1}^{\lfloor \frac{k}{2} \rfloor} (1 - 2^{1-2i})$ is decreasing to a limit approximate to 0.419, here $\lfloor \frac{k}{2} \rfloor$ is the maximal integer less or equal to $k/2$.

Similar distribution result for the congruent elliptic curves $E^{(n)}$ with rank 0 and $\text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^4$ is proved in Theorem 3. Now we explain the strategy to prove this theorem:

- By our previous paper [2]: $n \in P_k(x)$ can be characterized with 8-rank of ideal class group of $\mathbb{Q}(\sqrt{-n})$, then Jung-Yue [3] reduces this to quartic residue symbol;
- We count according to $p_i \pmod{16}$ and the residue symbol of prime factors of n , which is reduced to count the number of certain matrix over \mathbb{F}_2 by independence of residue symbol Theorem 2.

To explain the independence of residue symbol property, we first introduce some notations. For $d \in Q_k$ and q an integer such that $\left(\frac{q}{p}\right) = 1$ for all prime divisor p of d , we denote $\left(\frac{q}{d}\right)_4$ to be the quartic residue symbol defined in §2.2. For an odd integer a , we define $\left[\frac{2}{a}\right] = 1$ if $a \equiv \pm 5 \pmod{8}$ and 0 else. Let k be a positive integer, we denote $C_k(x)$ to be all positive square-free integers $n \leq x$ with exactly k prime divisors. Let $\alpha = (\alpha_1, \dots, \alpha_k)$ with $\alpha_l \in \{1, 5, 9, 13\}$ and $\prod_{l=1}^k \alpha_l \equiv 1 \pmod{8}$, and B be a $k \times k$ symmetric \mathbb{F}_2 -matrix with rank $k-1$ and every row sum 0. Then $\mathbf{b} = \left(\left[\frac{2}{\alpha_1}\right], \dots, \left[\frac{2}{\alpha_k}\right]\right)^T$ lies in the image of B viewed as a linear transform over \mathbb{F}_2^k . Moreover $By = \mathbf{b}$ has two different solutions $y, y' \in \mathbb{F}_2^k$ with $y + y' = (1, \dots, 1)^T$. We assume $z = (z_1, \dots, z_k)^T$ to be the one of y, y' such that $z_1 = 1$. Then we define $C_k(x, \alpha, B)$ to be all $n = p_1 \cdots p_k \in C_k(x)$ with $p_1 < \cdots < p_k$ satisfying the following conditions:

- $p_l \equiv \alpha_l \pmod{16}$ for $1 \leq l \leq k$;
- The Legendre symbol $\left(\frac{p_l}{p_j}\right) = (-1)^{B_{lj}}$ for all $1 \leq l < j \leq k$;
- $\left(\frac{2d}{n/d}\right)_4 \left(\frac{2n/d}{d}\right)_4 = (-1)^{\frac{n-1}{8} + \frac{d-5}{4}}$ with $d = \prod p_l^{z_l}$.

Now we can state the independence of residue symbol property:

Theorem 2. *Let $\alpha = (\alpha_1, \dots, \alpha_k)$ with $\alpha_l \in \{1, 5, 9, 13\}$ and $\prod_{l=1}^k \alpha_l \equiv 1 \pmod{8}$. Then for any $k \times k$ symmetric matrix B over \mathbb{F}_2 with every row sum 0 and rank $k-1$, we have*

$$\#C_k(x, \alpha, B) \sim \frac{1}{2^{3k + \binom{k}{2} + 1}} \cdot \#C_k(x)$$

where $\binom{k}{2}$ is the binomial coefficient and \sim means that the ratio of its two sides has limit 1 as x goes to infinity.

Rhoades [4] claimed a special case of above Theorem. Moreover he proved an independence of residue symbol property with the method of Cremona-Odoni [5] over \mathbb{Q} . For Theorem 2, we have to extend the method of Cremona-Odoni to $\mathbb{Q}(i)$ because of the quartic residue symbol, whence parallel results like the explicit formula for $\psi(x, \chi)$, Siegel Theorem and Page Theorem are needed. Moreover, we have to transit from primes to prime ideals and deal with some difficulty in counting certain residue classes, this can be best seen in the case $k=1$ (§3.1).

Since we will use analytic number theory, we will use many standard symbols in analytic number theory, such as $\sim, o(\cdot), O(\cdot), \ll, \pi(x), \text{Li}(x), \psi(x)$, they can be find in any book on analytic number theory, for example Iwaniec-Kowalski [7].

In the end of this introduction, we give the organization of this paper. We devote Section 2 to give some preliminary results. Concretely, in §2.1 we summarize the method of Cremona-Odoni in a simpler case; Since many residue symbols are used, we give their definition and prove some properties in §2.2; Those parallel analytic number theory results are enumerated in §2.3. With these preparation, we prove Theorem 2 in Section 3, especially we split out the case $k = 1$ to outstand the main difficulty beside the idea of Cremona-Odoni in §3.1. The distribution result is carried out in Section 4.

2 Preliminary Section

2.1 Basic Idea

Since the method of Cremona-Odoni [5] plays an important role in our proof of independence of residue symbol property. Now we explain their basic idea in a much simpler case:

$$\#C_k(x) \sim \frac{1}{(k-1)!} \cdot \frac{x}{\log x} \cdot (\log \log x)^{k-1}$$

where $C_k(x)$ denotes all square-free positive integer $n \leq x$ with exact k prime factors. For $k = 1$ this is prime number theorem.

For $k \geq 2$ their key idea is to consider the induction map

$$C_k(x) \xrightarrow{\varphi} C_{k-1}(x), n \mapsto n/\tilde{n}$$

where \tilde{n} is the maximal prime divisor of n . Note $t \in C_{k-1}(x)$ is in the image of φ if and only if there is a prime p such that $\tilde{t} < p \leq xt^{-1}$, thus we get:

$$\#C_k(x) = \sum_{t \in C_{k-1}(x)} \#\{p \text{ prime} \mid \tilde{t} < p \leq xt^{-1}\}$$

Then the following Lemma 3.1 of Cremona-Odoni [5] implies that only $t \in (\mu, \nu] \cap C_{k-1}(x)$ contributes to the main term of $\#C_k(x)$ with $\mu = (\log x)^{100}, \nu = \exp\left(\frac{\log x}{(\log \log x)^{100}}\right)$:

Lemma 1. *If either $m = 20, n = \mu$, or $m = \nu, n = x^{\frac{k-1}{k}}$, then we have:*

$$\begin{aligned} \sum_{m < t \leq n}^* \text{Li}(xt^{-1}) &= o\left(\frac{x \cdot (\log \log x)^{k-1}}{\log x}\right) \\ \sum_{\mu < t \leq \nu}^* \text{Li}(xt^{-1}) &\sim \frac{1}{k-1} \cdot \#C_{k-1}(x) \cdot \log \log x \end{aligned}$$

Where $\sum_{a < t \leq b}^* f(t) := \sum_{t \in (a, b] \cap C_{k-1}(\infty)} f(t)$.

Whence we reduce to estimate $\sum_{\mu < t \leq \nu}^* \pi(xt^{-1})$. From prime number theorem we only need to estimate $\sum_{\mu < t \leq \nu}^* \text{Li}(xt^{-1})$, then Lemma 1 and induction give

$$\#C_k(x) \sim \frac{1}{(k-1)!} \cdot \frac{x}{\log x} (\log \log x)^{k-1}$$

For the problem considered by Cremona-Odoni [5], they have to use $\psi(xt^{-1}, a, q)$ instead of $\pi(xt^{-1})$. This forces they have to use explicit formula of $\psi(x, \chi)$, which brings the additional difficulty to deal with possible Siegel zeros in the error term. Due to Page's Theorem, Siegel zeros are so rare that the sum of all the trivial estimation of $\psi(xt^{-1}, \chi)$ with possible Siegel zero contributes to an error term.

Comparing with Cremona-Odoni, we have to deal with corresponding multiplicative number theory over $\mathbb{Q}(i)$.

2.2 Residue Symbols

In this subsection, we will introduce several residue symbols that will be widely used in this paper.

For λ a prime in Gaussian integers $\mathbb{Z}[i]$ coprime with $1+i$ and α a Gaussian integer, the quartic residue symbol $(\frac{\alpha}{\lambda})_4$ is defined to be the unique element in $\{\pm 1, \pm i, 0\}$ such that

$$\alpha^{\frac{\lambda\bar{\lambda}-1}{4}} \equiv \left(\frac{\alpha}{\lambda}\right)_4 \pmod{\lambda}$$

holds over $\mathbb{Z}[i]$, where $\bar{\lambda}$ is the conjugate of λ . The reference is Ireland-Rosen [6].

For two Gaussian primes λ_1, λ_2 , we easily deduce that

$$\left(\frac{\lambda_1}{\lambda_2}\right)_4 \left(\frac{\bar{\lambda}_1}{\lambda_2}\right)_4 = 1$$

Moreover, we have the quartic reciprocity law

$$\left(\frac{\lambda_1}{\lambda_2}\right)_4 = \left(\frac{\lambda_2}{\lambda_1}\right)_4 (-1)^{\frac{N\lambda_1-1}{4} \frac{N\lambda_2-1}{4}}$$

where N denotes the norm from $\mathbb{Q}(i)$ to \mathbb{Q} . If $\theta = \prod_{l=1}^k \lambda_l$ with λ_l prime and coprime with $1+i$, we define

$$\left(\frac{\alpha}{\theta}\right)_4 = \prod_{l=1}^k \left(\frac{\alpha}{\lambda_l}\right)_4$$

We say an integer $\theta \in \mathbb{Z}[i]$ is primary if $\theta \equiv 1 \pmod{2+2i}$. Since we will frequently consider $(\frac{2}{\theta})_4$, we compute it in the following lemma:

Lemma 2. *If $\theta = a + 2bi$ is a primary integer with $a, b \in \mathbb{Z}$, then $(\frac{2}{\theta})_4 = i^{-b}$.*

Proof. If θ has rational prime factor p congruent to 3 (mod 4), then $(\frac{2}{-p})_4 = 1$ and there must be even many such factors counted with multiplicity, so their product is congruent to 1 (mod 4). Hence we reduce to show that θ has only Gaussian prime factors.

Now we induct on the prime factors of θ . If θ is a prime, then $(\frac{2}{\theta})_4 = i^{-b}$, see P53 of Iwaniec-Kowalski [7]. For θ has $k \geq 2$ prime factors, then $\theta = \theta_1 \theta_2$ with θ_l a primary Gaussian integer having less than k prime factors for $l = 1, 2$. Hence if we denote $\theta_l = a_l + 2b_l i$ with $a_l, b_l \in \mathbb{Z}$, then induction implies that

$$\left(\frac{2}{\theta_l}\right)_4 = i^{-b_l}$$

Hence $(\frac{2}{\theta})_4 = i^{-(b_1+b_2)}$ by definition. On the other hand,

$$a + 2bi = \theta = \theta_1 \theta_2 = a_1 a_2 - 4b_1 b_2 + 2(a_1 b_2 + a_2 b_1)i$$

Therefore $b = a_1 b_2 + a_2 b_1$. Since θ_l is primary, we have $a_l - 2b_l \equiv 1 \pmod{4}$. Consequently $b \equiv (1 + 2b_1)b_2 + (1 + 2b_2)b_1 \equiv b_1 + b_2 \pmod{4}$. So by induction, the Lemma is proved. \square

For p a prime congruent to 1 (mod 4), there are exactly two primitive primes $\lambda, \bar{\lambda}$ lying above p with $p = \lambda\bar{\lambda}$. For q a rational integer with $\left(\frac{p}{q}\right) = 1$, then the two quartic residue symbol $\left(\frac{q}{\lambda}\right)_4 = \left(\frac{q}{\bar{\lambda}}\right)_4 = \pm 1$. Then we use the symbol $\left(\frac{q}{p}\right)_4$ to denote $\left(\frac{q}{\lambda}\right)_4$ as in Jung-Yue [3]. Note this symbol has the convenience that we needn't choose which primary prime above p . Moreover if d is a positive integer with all prime factors congruent to 1 (mod 4), and q such that $\left(\frac{q}{p}\right) = 1$ for any prime factor p of d , then

$$\left(\frac{q}{d}\right)_4 := \prod_{p|d} \left(\frac{q}{p}\right)_4^{v_p(d)}$$

where $v_p(d)$ denotes the p -adic valuation of d .

For future application, we introduce general Legendre symbol over $\mathbb{Z}[i]$ as in Page 196 of Hecke [8]: Let \mathfrak{p} be a prime ideal coprime with $(1+i)$, the general Legendre symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)$ is defined to be the unique element of $\{\pm 1, 0\}$ such that

$$\alpha^{\frac{N_{\mathfrak{p}}-1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right) \pmod{\mathfrak{p}}$$

holds. If λ is the unique primary prime in \mathfrak{p} , we also denote

$$\left(\frac{\alpha}{\lambda}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)$$

If $\theta = \prod_{l=1}^k \lambda_l$ with λ_l primary prime, we denote

$$\left(\frac{\alpha}{\theta}\right) = \prod_{l=1}^k \left(\frac{\alpha}{\lambda_l}\right)$$

Another residue symbol is needed, for p a rational prime and a a rational integer coprime with p , the additive Legendre symbol $\left[\frac{a}{p}\right]$ is 1 if the Legendre symbol $\left(\frac{a}{p}\right) = -1$, else it is 0. Similarly for d a positive odd integer, we denote $\left[\frac{a}{d}\right] = 1$ if the Jacobi symbol $\left(\frac{a}{d}\right) = -1$ and $\left[\frac{a}{d}\right] = 0$ if $\left(\frac{a}{d}\right) = 1$.

2.3 Analytic results over number fields

Let K be a number field of degree n with discriminant Δ and ring of algebraic integers \mathcal{O} . A non-zero element $\gamma \in K$ is totally positive if it is positive under all real embeddings. If K has no real embedding, then totally positive means non-zero. For an integral ideal \dagger and $\gamma \in K$, the notation $\gamma \equiv 1 \pmod{\dagger}$ means that $\gamma \in \mathcal{O}_{\mathfrak{p}}$ and $\gamma \equiv 1 \pmod{\mathfrak{p}^{v_{\mathfrak{p}}(\dagger)}}$ if $\mathfrak{p} \mid \dagger$, where $\mathcal{O}_{\mathfrak{p}}$ is the integer ring of the \mathfrak{p} -adic completion of K . Let P_{\dagger} be the group of principal fractional ideals (γ) with γ totally positive and $\gamma \equiv 1 \pmod{\dagger}$, and $I(\dagger)$ denote the set of all the fractional ideals that are coprime with \dagger . We say χ is a character modulo an ideal \dagger if χ is a character induced from $I(\dagger)/P_{\dagger}$. Then $\psi(x, \chi)$ is defined to be

$$\psi(x, \chi) = \sum_{N_K \mathfrak{a} \leq x} \chi(\mathfrak{a}) \Lambda(\mathfrak{a})$$

where \mathfrak{a} runs over all the integral ideal with norm less than or equal to x and N_K denotes the norm from K to \mathbb{Q} , and $\Lambda(\mathfrak{a})$ is the Mangoldt function

$$\begin{cases} \log N_K \mathfrak{p} & \text{if } \mathfrak{a} = \mathfrak{p}^m \text{ with } m \geq 1, \\ 0 & \text{else.} \end{cases}$$

and $\chi(\mathfrak{a}) = 0$ if \mathfrak{a} is not coprime with \dagger . For $\psi(x, \chi)$, we have the following explicit formula (see Iwaniec-Kowalski [7] P114):

Proposition 1.

For χ a non-principal character mod \dagger and $1 \leq T \leq x$, then

$$\psi(x, \chi) = - \sum_{|\text{Im} \rho| \leq T} \frac{x^\rho - 1}{\rho} + O\left(xT^{-1} \cdot \log x \cdot \log(x^n \cdot N\dagger)\right) \quad (2.1)$$

where ρ runs over all the zeros of $L(s, \chi)$ with $0 \leq \text{Re} \rho \leq 1$ and $|\text{Im} \rho| \leq T$, and the implied constant depends only on K .

For further application, we introduce Siegel's Theorem and Page's Theorem over K . For Siegel's Theorem over K , we refer to Fogels [9], [10], [11], while for Page's Theorem over K we refer to Hoffstein-Ramakrishnan [12].

Proposition 2. (1) For χ a character modulo \dagger , and $D = |\Delta|N\dagger > D_0 > 1$,

(i) there is a positive constant c (which only depends on n) such that in the region

$$\text{Re}(s) > 1 - \frac{c}{\log D(1 + |\text{Im}(s)|)} > \frac{3}{4} \quad (*)$$

there is no zero of $L(s, \chi)$ with χ complex, for at most one real χ' there maybe a simple zero β' of $L(s, \chi')$;

(ii) If β' is the exceptional zero of the exceptional character χ' modulo \dagger , then for any $\epsilon > 0$, there is a positive constant $c(n, \epsilon)$ such that

$$1 - \beta' > c(n, \epsilon)D^{-\epsilon}$$

(2) For any $z \geq 2$, and c_0 is a suitable constant, then there is at most a real primitive character χ to a modulus \dagger with $N_K\dagger \leq z$ has a real zero β satisfying

$$\beta > 1 - \frac{c_0}{\log z}$$

For future purpose, the first term of the formula (2.1) have to be estimated. Similar as classical case, we can get the following explicit version of formula (2.1).

$$\psi(x, \chi) = - \frac{x^{\beta'}}{\beta'} + R(x, T) \quad (2.2)$$

with

$$R(x, T) \ll x \cdot \log^2(x \cdot N_K\dagger) \cdot \exp\left(-\frac{c_1 \log x}{\log |T \cdot N_K\dagger|}\right) + xT^{-1} \log x \cdot \log \left|x^n \cdot N_K\dagger\right| + x^{\frac{1}{4}} \log x$$

The term $-\frac{x^{\beta'}}{\beta'}$ occurs only if χ is a real character for which has a zero β' (then must be unique and simple) with

$$\beta' > 1 - \frac{c_2}{\log N_K\dagger}$$

where c_2 is a certain constant.

3 Independence of residue symbol property

To prove independence of residue symbol Theorem 2, we have to identify the set $C_k(x, \alpha, B)$ to a set counts certain integers over $\mathbb{Q}(i)$. For this purpose, we introduce some notations.

Denote \mathcal{P} to be the set of all primary primes in $\mathbb{Z}[i]$ with imaginary part positive. Let $k \geq 1$, and $\alpha = (\alpha_1, \dots, \alpha_k)$ with $\alpha_l \in \{1, 5, 9, 13\}$ and $\prod_{l=1}^k \alpha_l \equiv 1 \pmod{8}$. For $B = B_{k \times k}$ a symmetric \mathbb{F}_2 -matrix with rank $k - 1$ and every row sum 0, we define $C'_k(x, \alpha, B)$ to be all $\eta = \prod_{l=1}^k \lambda_l$ satisfying

- $N\lambda_1 < \dots < N\lambda_k$ with $\lambda_l \in \mathcal{P}$ and $N\eta \leq x$;
- $N\lambda_l \equiv \alpha_l \pmod{16}$ and $\left(\frac{N\lambda_l}{N\lambda_j}\right) = (-1)^{B_{lj}}$ for all $l < j$;
- $\left(\frac{\theta_2}{\theta_1}\right)_4 \left(\frac{2}{\eta}\right)_4 = (-1)^{\frac{\prod_1^k \alpha_j - 1}{8} + \frac{\prod_1^k \alpha_j^{z_j} - 5}{4}}$ where $\theta_1 \theta_2 = \eta$ and $\theta_1 = \prod_{l=1}^k \lambda_l^{z_l}$.

where $z = (z_1, \dots, z_k)^T \in \mathbb{F}_2^k$ satisfying $Bz = \left(\left[\frac{2}{\alpha_1}\right], \dots, \left[\frac{2}{\alpha_k}\right]\right)^T$ with $z_1 = 1$.

For $n = p_1 \dots p_k \in C_k(x, \alpha, B)$ with p_l arranged increasingly, and for any p_l we chose the unique $\lambda_l \in \mathcal{P}$ such that $p_l = \lambda_l \bar{\lambda}_l$. Then we claim that $\eta = \prod_{l=1}^k \lambda_l \in C'_k(x, \alpha, B)$. Note that η obviously satisfies the first and second conditions in defining $C'_k(x, \alpha, B)$. For the third: consider the l -th row of both sides of $Bz = \left(\left[\frac{2}{p_1}\right], \dots, \left[\frac{2}{p_k}\right]\right)^T$, we get

$$\sum_{j=1, j \neq l}^k z_j B_{lj} + z_l \sum_{j=1, j \neq l}^k B_{lj} = \left[\frac{2}{p_l}\right], \quad B_{lj} = \left[\frac{p_j}{p_l}\right] \text{ if } j \neq l$$

since every row sum of B is 0. Then we have $\left(\frac{2n/d}{p_l}\right) = 1$ if $z_l = 1$ and $\left(\frac{2d}{p_l}\right) = 1$ if $z_l = 0$. Thus the notations $\left(\frac{2d}{n/d}\right)_4, \left(\frac{2d}{n/d}\right)_4$ are meaningful, according to their definition we have:

$$\begin{aligned} \left(\frac{2n/d}{d}\right)_4 \left(\frac{2d}{n/d}\right)_4 &= \left(\frac{2p_{t+1} \dots p_k}{\lambda_1 \dots \lambda_t}\right)_4 \left(\frac{2p_1 \dots p_t}{\lambda_{t+1} \dots \lambda_k}\right)_4 \\ &= \left(\frac{2}{\eta}\right)_4 \cdot \prod_{l=1}^t \prod_{j=t+1}^k \left(\frac{p_j}{\lambda_l}\right)_4 \left(\frac{p_l}{\lambda_j}\right)_4 \\ &= \left(\frac{2}{\eta}\right)_4 \cdot \prod_{l=1}^t \prod_{j=t+1}^k \left(\frac{\lambda_j}{\lambda_l}\right)_4 \left(\frac{\bar{\lambda}_j}{\bar{\lambda}_l}\right)_4 \left(\frac{\lambda_l}{\lambda_j}\right)_4 \left(\frac{\bar{\lambda}_l}{\bar{\lambda}_j}\right)_4 \end{aligned}$$

where we have assumed that $d = p_1 \dots p_t$ for simplicity of notation. Using quartic reciprocity law for $\left(\frac{\lambda_l}{\lambda_j}\right)_4$ and $\left(\frac{\bar{\lambda}_l}{\bar{\lambda}_j}\right)_4$ we get

$$\left(\frac{\lambda_j}{\lambda_l}\right)_4 \left(\frac{\bar{\lambda}_j}{\bar{\lambda}_l}\right)_4 \left(\frac{\lambda_l}{\lambda_j}\right)_4 \left(\frac{\bar{\lambda}_l}{\bar{\lambda}_j}\right)_4 = \left(\frac{\lambda_j}{\lambda_l}\right)_4 \left(\frac{\bar{\lambda}_j}{\bar{\lambda}_l}\right)_4 \left(\frac{\lambda_j}{\bar{\lambda}_l}\right)_4$$

From $\left(\frac{\bar{\lambda}_j}{\lambda_l}\right)_4 \left(\frac{\lambda_j}{\bar{\lambda}_l}\right)_4 = 1$ we obtain

$$\left(\frac{2n/d}{d}\right)_4 \left(\frac{2d}{n/d}\right)_4 = \left(\frac{2}{\eta}\right)_4 \left(\frac{\theta_2}{\theta_1}\right)_4 \quad (3.1)$$

Thus $\eta \in C'_k(x, \alpha, B)$. From this we obtain a bijection

$$C_k(x, \alpha, B) \rightarrow C'_k(x, \alpha, B) \quad (3.2)$$

Now we divide the proof of Theorem 2 into two cases according to $k = 1$ or not. The reason is twofold: First this case will not use the method of Cremona-Odoni, second we can see the main difference between Cremona-Odoni and our situation, which makes the proof of the case $k \geq 2$ more natural and not too long.

3.1 The case $k = 1$

For the case $k = 1$, then we have $\alpha_1 \in \{1, 9\}$. Moreover only $B = 0_{1 \times 1}$ has rank $k - 1 = 0$, so $C'_1(x, \alpha_1, 0)$ consists all primary primes $\lambda \in \mathcal{P}$ such that:

$$N\lambda \leq x, \quad N\lambda \equiv \alpha_1 \pmod{16}, \quad \left(\frac{2}{\lambda}\right)_4 = (-1)^{\frac{\alpha_1 - 9}{8}}$$

If we let A_{16} be those primary classes a of $\mathbb{Z}[i]/16\mathbb{Z}[i]$ such that

$$(i) \quad Na \equiv \alpha_1 \pmod{16};$$

$$(ii) \quad \left(\frac{2}{a}\right)_4 = (-1)^{\frac{\alpha_1 - 9}{8}}.$$

then by Lemma 2 we yield

$$\#C'_1(x, \alpha_1, 0) = \frac{1}{2}\pi'(x, A_{16}, 16) \quad (3.3)$$

where $\pi'(y, A, \gamma)$ is the number of primes λ in $\mathbb{Z}[i]$ with $N\lambda \leq y$ and $\lambda \in A \pmod{\gamma}$, and the additional factor $\frac{1}{2}$ comes from $\lambda \in C'_1(x, \alpha, 0)$ with positive imaginary part.

Since Dirichlet prime ideal Theorem over $\mathbb{Q}(i)$ concerns prime ideals while our estimation concerns prime elements, we have to bridge this gap by the following: Let \mathfrak{c} be the ideal $16\mathbb{Z}[i]$, then by Theorem 6.1 of Lang [13] we have the following long exact sequence:

$$1 \longrightarrow \mathbb{Z}[i]^\times \longrightarrow \left(\mathbb{Z}[i]/\mathfrak{c}\right)^\times \xrightarrow{f} I(\mathfrak{c})/P_{\mathfrak{c}} \longrightarrow 1 \quad (3.4)$$

where f is induced by mapping every \mathfrak{c} -invertible Gauss integer a to the class generated by (a) . In fact, the exactness of (3.4) can be verified directly using $\mathbb{Z}[i]$ having class number 1. Furthermore, we introduce the notation $\pi(y, \mathfrak{A}, \mathfrak{a})$ to denote all those prime ideal lies in the classes \mathfrak{A} modulo $P_{\mathfrak{a}}$ with norm less or equal to y .

Now we can transit to prime ideals: let \mathfrak{A}_{16} be the image of A_{16} under f , then we get

$$\pi'(x, A_{16}, 16) = \pi(x, \mathfrak{A}_{16}, \mathfrak{c}) \quad (3.5)$$

This is because for any prime ideal (λ) in the class of \mathfrak{A}_{16} , there are exactly four primes lie in (λ) but with exact one of them primary, whence

$$\#\mathfrak{A}_{16} = \#A_{16} \quad (3.6)$$

From Dirichlet prime ideal theorem over $\mathbb{Q}(i)$ (see Proposition 1), we get

$$\pi(x, \mathfrak{A}_{16}, \mathfrak{c}) \sim \frac{\#\mathfrak{A}_{16}}{\#I(\mathfrak{c})/P_{\mathfrak{c}}} \cdot \text{Li}(x)$$

Let $\phi(16)$ be the number of $(\mathbb{Z}[i]/16\mathbb{Z}[i])^\times$, then from the exact sequence (3.4) we have $\#I(\mathfrak{c})/P_{\mathfrak{c}} = \frac{\phi(16)}{4}$, whence from (3.3) and (3.5) we obtain:

$$\#C'_1(x, \alpha_1, 0) \sim \frac{2\#\mathfrak{A}_{16}}{\phi(16)} \cdot \text{Li}(x)$$

Then according to the following Lemma 3, we get

$$\#C'_1(x, \alpha_1, 0) \sim \frac{1}{2^4} \cdot \text{Li}(x)$$

Note $\#C_1(x) \sim \text{Li}(x)$ and the bijection (3.2), we finish the proof of Theorem 2 in the case $k = 1$.

Lemma 3. *The cardinality of A_{16} is $\phi(16)/2^5$.*

Proof. By the definition of A_{16} , the class is primary selects the subgroup $G = \overline{1 + (2 + 2i)\mathbb{Z}[i]}$ of the group $(\mathbb{Z}[i]/16\mathbb{Z}[i])^\times$ which is four times of G in cardinality. To determine those elements in G selected by the conditions (i),(ii) we introduce two characters χ_j on G defined by:

$$\chi_1(g) = i^{\frac{Ng-1}{4}}, \quad \chi_2(g) = \left(\frac{2}{g}\right)_4$$

Then conditions (i),(ii) are equivalent to find those $g \in G$ such that

$$\chi_1(g) = i^{\frac{\alpha_1-1}{4}}, \quad \chi_2(g) = (-1)^{\frac{\alpha_1-9}{8}} \quad (3.7)$$

This reminds us to study the behavior of χ_i over G . We can easily deduce that $\chi_j^2(g) = \left(\frac{2}{Ng}\right)$ with $j = 1, 2$. Whence $\chi_1^2 = \chi_2^2$ and they are characters of order 4, since $\chi_j^2(-1 + 2i) = -1$. Moreover we have $\chi_1(-1 + 2i) = i, \chi_2(-1 + 2i) = i^{-1}$ by Lemma 2. Therefore $\chi_1 \neq \chi_2$. So the character subgroup G' generated by χ_1, χ_2 has 8 elements.

Now we show that G' is the dual group of $G/G_1 \cap G_2$ with G_i the kernel of χ_i . We suffice to prove $\#G/G_1 \cap G_2 = 8$. From group isomorphism theorem, we only need to study G/G_1 and $G_1/G_1 \cap G_2$. The first group $G/G_1 \simeq \mu_4$ as χ_1 has order 4, for the latter group we have $\chi_2|_{G_1} : G_1/G_1 \cap G_2 \rightarrow \mu_4$, where μ_4 is the group of units of order 4. Due to $\chi_1 \neq \chi_2$ we know $\chi_2|_{G_1}$ is non-trivial. From $\chi_1^2 = \chi_2^2$ we obtain

$$\chi_2(g_1)^2 = \chi_1(g_1^2) = 1, \quad g_1 \in G_1$$

Whence $\chi_2|_{G_1}$ has order 2 and $\#G_1/G_1 \cap G_2 = 2$. Thus we get $\#G/G_1 \cap G_2 = 8$. Therefore G' is the dual group of $G/G_1 \cap G_2$ by counting cardinality.

Since G' and $G/G_1 \cap G_2$ are dual groups, we can easily derive: there is a $g \in G$ with $\chi_j(g) = i^{x_j}$ for $j = 1, 2$ if and only if $i^{2x_1} = i^{2x_2}$ since $\chi_1^2 = \chi_2^2$. Note that $i^{\frac{\alpha_1-1}{4}}, (-1)^{\frac{\alpha_1-9}{8}}$ obviously satisfies this. Therefore there is a $g_0 \in G$ such that (3.7) holds. Moreover by transition of g_0 , we know all $g \in G$ satisfying (3.7) consists the subset $g_0(G_1 \cap G_2)$, which selects an eighth of G .

$$\#A_{16} = \frac{\phi(16)}{2^5}$$

This completes the proof of the lemma. \square

3.2 The case $k \geq 2$

In this subsection we will use the method of Cremona-Odoni to prove Theorem 2 with $k \geq 2$.

To define the similar map φ as in §2, we first define $T(x)$ to be all $n = p_1 \cdots p_{k-1} \leq x$ with p_j arranged in ascending order such that

$$p_l \equiv \alpha_l \pmod{16}, \left(\frac{p_l}{p_j} \right) = (-1)^{B_{lj}}, 1 \leq l < j \leq k-1$$

From independence of Legendre symbol property of Rhoades [4], we have

$$\#T(x) \sim 2^{-\binom{k}{2}-2k+2} \cdot \#C_{k-1}(x) \quad (3.8)$$

Similarly as $C'_k(x, \alpha, B)$ we define $T'(x)$ to be all $\eta = \lambda_1 \cdots \lambda_{k-1}$ with $N\eta \leq x$ and $\lambda_j \in \mathcal{P}$ such that

$$N\lambda_j \equiv \alpha_j \pmod{16}, \left(\frac{N\lambda_l}{N\lambda_j} \right) = (-1)^{B_{lj}}, 1 \leq l < j \leq k-1$$

where we have arranged $N\lambda_l$ increasingly. Then we also have a bijection

$$T'(x) \longrightarrow T(x), \quad \eta \mapsto N\eta \quad (3.9)$$

Now we can prove Theorem 2:

Proof. Let $\tilde{\eta} \in \mathcal{P}$ be the prime divisor of η with maximal norm, then we define the map

$$\varphi : C'_k(x, \alpha, B) \rightarrow T'(x), \quad \eta \mapsto \eta/\tilde{\eta}$$

parallel as in §2. Now we divide into two cases according to $z_k = 0$ or 1.

For the case $z_k = 0$: we know an $\epsilon = \prod_1^{k-1} \lambda_j \in T'(x)$ lies in the image of φ if and only if there is a prime $\lambda \in \mathcal{P}$ with $N\tilde{\epsilon} < N\lambda \leq x/N\epsilon$ such that

$$(i): N\lambda \equiv \alpha_k \pmod{16} \text{ and } \left(\frac{N\lambda}{N\lambda_j} \right) = (-1)^{B_{jk}} \text{ with } 1 \leq j \leq k-1;$$

$$(ii): \left(\frac{2}{\lambda} \right)_4 \left(\frac{\lambda}{\theta_1} \right) = \left(\frac{2}{\epsilon} \right)_4 \left(\frac{\epsilon/\theta_1}{\theta_1} \right) (-1)^{\frac{\Pi_1^k \alpha_{j-1}}{8} + \frac{\Pi_1^k \alpha_j^{z_j} - 5}{4}}.$$

here $\tilde{\epsilon} \in \mathcal{P}$ is the prime divisor of ϵ with maximal norm.

Thus from Lemma 2, there is a unique subset A_ϵ of invertible primary residue classes modulo 16ϵ such that for a prime λ : the integer $\lambda\epsilon$ belongs to $C'_k(x, \alpha, B)$ if and only if λ lies in \mathcal{P} and $A_\epsilon \pmod{16\epsilon}$ with norm in $(N\tilde{\epsilon}, x/N\epsilon]$. Whence we obtain

$$\#C'_k(x, \alpha, B) = \sum_{\epsilon \in T'(x)} g(\epsilon) \quad (3.10)$$

with

$$g(\epsilon) = \# \left\{ \lambda \text{ prime of } \mathbb{Z}[i] \mid \lambda \in \mathcal{P}, \lambda \in A_\epsilon \pmod{16\epsilon}, N\tilde{\epsilon} < N\lambda \leq x/N\epsilon \right\}$$

As $\#A_\epsilon$ is an important part in main term, we list in the following lemma with proof postponed in the end of this section.

Lemma 4. Let $\phi(16\epsilon)$ be the number of $\left(\mathbb{Z}[i]/16\epsilon\mathbb{Z}[i]\right)^\times$, then

$$\#A_\epsilon = \frac{\phi(16\epsilon)}{2^{k+4}}$$

For simplicity, we introduce the notation $\sum_{N\eta \in A}^* f(\eta)$ to denote $\sum_{\eta \in T(\infty), N\eta \in A} f(\eta)$ when $A \subset \mathbb{N}$ as Cremona-Odoni. Similarly as Cremona-Odoni, a Lemma parallel to Lemma 1 also holds if we use T' to substitute C_{k-1} , and μ, ν are defined the same as Lemma 1.

Now we can estimate $\#C'_k(x, \alpha, B)$ in equation (3.10):

First for $\epsilon \in T(x)$ with $N\epsilon \leq 20$, then :

$$g(\epsilon) \leq \pi(x/N\epsilon)$$

since every prime ideal corresponds to exact 1 primitive prime elements, where

$$\pi(y) = \sum_{N\mathfrak{p} \leq y} 1 \sim \text{Li}(y)$$

by prime ideal Theorem over $\mathbb{Q}(i)$. So all these ϵ with $N\epsilon \leq 20$ contribute at most $O\left(\frac{x}{\log x}\right)$.

Second for $N\epsilon$ lies in $(20, \mu]$: similarly we have

$$g(\epsilon) = O\left(\text{Li}(x/N\epsilon)\right)$$

Hence these ϵ contributes to

$$\sum_{20 < t \leq \mu} O\left(\text{Li}(xt^{-1})\right) = O\left(\sum_{20 < t \leq \mu} \text{Li}(xt^{-1})\right) = o\left(\frac{x}{\log x} \cdot (\log \log x)^{k-1}\right)$$

by Lemma 1.

Similarly for $N\epsilon$ belonging to $(\nu, x^{\frac{k-1}{k}}]$, they also contribute to $o\left(\frac{x}{\log x} \cdot (\log \log x)^{k-1}\right)$.

While for those $N\epsilon > x^{\frac{k-1}{k}}$, they have no contribution: as in this case we have $N\tilde{\epsilon} > x^{\frac{1}{k}}$, but this contradicts that $N\tilde{\epsilon} < N\lambda \leq x/N\epsilon < x^{\frac{1}{k}}$.

Consequently we obtain:

$$\#C'_k(x, \alpha, B) \sim \frac{1}{2} \sum_{\mu < N\epsilon \leq \nu}^* \left(\pi'(x/N\epsilon, A_\epsilon, 16\epsilon) - \pi'(N\tilde{\epsilon}, A_\epsilon, 16\epsilon) \right)$$

Recall that $\pi'(y, A, \gamma)$ is defined under (3.3). For the contribution of above latter terms we yield:

$$\sum_{\mu < N\epsilon \leq \nu}^* \pi'(N\tilde{\epsilon}, A_\epsilon, 16\epsilon) \leq \nu \cdot O\left(\frac{\nu}{\log \nu}\right) = O\left(\frac{\nu^2}{\log \nu}\right) = o\left(\frac{x}{\log x} \cdot (\log \log x)^{k-1}\right)$$

Therefore we have

$$\#C'_k(x, \alpha, B) \sim \frac{1}{2} \sum_{\mu < N\epsilon \leq \nu}^* \pi'(x/N\epsilon, A_\epsilon, 16\epsilon) \quad (3.11)$$

Similar as the case $k = 1$, we define $\mathfrak{c} = \mathfrak{c}_\epsilon$ to be the ideal generated by 16ϵ , then we have the following long exact sequence:

$$1 \longrightarrow \mathbb{Z}[i]^\times \longrightarrow \left(\mathbb{Z}[i]/\mathfrak{c}\right)^\times \xrightarrow{f} I(\mathfrak{c})/P_\mathfrak{c} \longrightarrow 1 \quad (3.12)$$

If we denote $\mathfrak{A}_\epsilon = f(A_\epsilon)$, then similarly as (3.5) and (3.6) we get

$$\pi'(x, A_\epsilon, 16\epsilon) = \pi(x, \mathfrak{A}_\epsilon, \mathfrak{c})$$

and

$$\#\mathfrak{A}_\epsilon = \#A_\epsilon \quad (3.13)$$

with $\pi(x, \mathfrak{A}_\epsilon, \mathfrak{c})$ defined under (3.4). Hence by equation (3.11) we reduce to estimate:

$$\sum_{\mu < N\epsilon \leq \nu}^* \pi(x/N\epsilon, \mathfrak{A}_\epsilon, \mathfrak{c})$$

Then by the standard relation of $\pi(y, \mathfrak{A}, \mathfrak{c})$ and $\psi(y, \mathfrak{A}, \mathfrak{c})$, we only need to estimate

$$\sum_{\mu < N\epsilon \leq \nu}^* \psi(x/N\epsilon, \mathfrak{A}_\epsilon, \mathfrak{c}) \quad (3.14)$$

where

$$\psi(y, \mathfrak{A}, \mathfrak{c}) := \sum_{\substack{N\mathfrak{a} \leq y \\ \mathfrak{a} \in \mathfrak{A} \bmod P_{\mathfrak{c}}}} \Lambda(\mathfrak{a})$$

By orthogonality of characters and above exact sequence (3.12), we have

$$\psi(y, \mathfrak{A}_\epsilon, \mathfrak{c}) = \frac{4}{\phi(16\epsilon)} \sum_{\chi \bmod \mathfrak{c}_\epsilon} \psi(y, \chi) \sum_{[\mathfrak{a}] \in \mathfrak{A}_\epsilon} \overline{\chi(\mathfrak{a})}$$

where χ runs over all the characters of $I(\mathfrak{c})/P_{\mathfrak{c}}$, and

$$\psi(y, \chi) := \sum_{N\mathfrak{a} \leq y} \chi(\mathfrak{a}) \Lambda(\mathfrak{a})$$

Consequently we divide the sum (3.14) into three parts according to principal characters, non-principal characters of modulus multiple of \dagger_1 or not:

$$\begin{aligned} \sum_{\mu < N\epsilon \leq \nu}^* \psi(x/N\epsilon, \mathfrak{A}_\epsilon, \mathfrak{c}) &= (I) + (II) + (III) \\ (I) &= \sum_{\mu < N\epsilon \leq \nu}^* \frac{4}{\phi(16\epsilon)} \cdot \#\mathfrak{A}_\epsilon \cdot \psi(x/N\epsilon, \chi_0) \\ (II) &= \sum_{\substack{\mu < N\epsilon \leq \nu, \\ \dagger_1 | \mathfrak{c}_\epsilon}}^* \frac{4}{\phi(16\epsilon)} \sum_{\chi \bmod \mathfrak{c}_\epsilon}' \psi(x/N\epsilon, \chi) \sum_{[\mathfrak{a}] \in \mathfrak{A}_\epsilon} \overline{\chi(\mathfrak{a})} \\ (III) &= \sum_{\substack{\mu < N\epsilon \leq \nu, \\ \dagger_1 \nmid \mathfrak{c}_\epsilon}}^* \frac{4}{\phi(16\epsilon)} \sum_{\chi \bmod \mathfrak{c}_\epsilon}' \psi(x/N\epsilon, \chi) \sum_{[\mathfrak{a}] \in \mathfrak{A}_\epsilon} \overline{\chi(\mathfrak{a})} \end{aligned}$$

where \dagger_1 is the conductor of the exceptional primitive character in (2) of Proposition 2 with $z = 16^2\nu$, and \sum' denotes all non-principal characters of a fixed modulus. These sums are estimated in the following lemma

Lemma 5.

$$\begin{aligned}
(I) &\sim \frac{1}{(k-1) \cdot 2^{k+2}} \cdot \#T'(x) \cdot \log x \cdot \log \log x \\
(II) &= O\left(x \log^{-99} \nu\right) \\
(III) &= o\left(\frac{x}{\log x}\right)
\end{aligned}$$

We postpone the proof of this Lemma. From this Lemma and the bijection (3.9) we arrive at:

$$\sum_{\mu < N\epsilon \leq \nu}^* \psi(x/N\epsilon, \mathfrak{A}_\epsilon, \mathfrak{c}) \sim \frac{1}{(k-1) \cdot 2^{k+2}} \cdot \#T(x) \cdot \log x \cdot \log \log x$$

Whence from the equations (3.8) and (3.11) we have

$$\begin{aligned}
\#C'_k(x, \alpha, B) &\sim \frac{1}{(k-1) \cdot 2^{k+3}} \cdot \#T(x) \cdot \log \log x \\
&\sim \frac{1}{(k-1) \cdot 2^{\binom{k}{2}+3k+1}} \cdot \log \log x \cdot \#C_{k-1}(x) \\
&\sim \frac{1}{2^{\binom{k}{2}+3k+1}} \cdot \#C_k(x)
\end{aligned}$$

For the case $z_k = 1$ we can prove similarly. Thus we complete the proof of Theorem 2 by noting the bijection (3.2). \square

Now we prove Lemma 5:

Proof. The first sum (I): by equation (3.13) and Lemma 4, we have $\#\mathfrak{A}_\epsilon = \frac{\phi(16\epsilon)}{2^{k+4}}$. Then Lemma 1 implies

$$\begin{aligned}
(I) &= \frac{1}{2^{k+2}} \sum_{\mu < N\epsilon \leq \nu}^* \psi(x/N\epsilon) = \frac{1+o(1)}{2^{k+2}} \sum_{\mu < N\epsilon \leq \nu}^* \log(x/N\epsilon) \text{Li}(x/N\epsilon) \\
&= \frac{1+o(1)}{2^{k+2}} \cdot \log x \sum_{\mu < N\epsilon \leq \nu}^* \text{Li}(x/N\epsilon) \\
&\sim \frac{1}{(k-1) \cdot 2^{k+2}} \cdot \#T'(x) \cdot \log x \cdot \log \log x
\end{aligned}$$

For the second sum (II): the trivial estimation gives:

$$(II) \ll \sum_{\substack{\mu < N\epsilon \leq \nu, \\ \dagger_1 | \epsilon_\epsilon}}^* \psi(x/N\epsilon) \ll x \sum_{\substack{\mu < N\epsilon \leq \nu, \\ \dagger_1 | \epsilon_\epsilon}}^* (N\epsilon)^{-1}$$

If we denote $\dagger_1 = \left((1+i)^e \beta_1 \cdots \beta_t\right)$ with $e \leq 8, t \leq k-1$ and $\beta_j \in \mathcal{P}$, then for any s with $\mu < sN\dagger_1 \leq \nu$ there are exactly 2^{k-1-t} ideals \mathfrak{c}' above s with $\dagger_1 \mathfrak{c}' = \mathfrak{c}_\epsilon$ for some $\epsilon \in T'(\infty)$. Therefore

$$(II) \ll xN\dagger_1^{-1} \sum_{\mu < sN\dagger_1 \leq \nu}^* s^{-1} \leq xN\dagger_1^{-1} \cdot \log \nu \quad (3.15)$$

But we we may assume that

$$N\mathfrak{f}_1 > (\log \nu)^{100}$$

As from Page Theorem part of Proposition 2, we chose $z = 16^2\nu$, then if the Siegel zero exists, we have the Siegel zero β of modulus \mathfrak{f}_1 satisfying

$$\beta > 1 - \frac{c_0}{\log(16^2\nu)}$$

Then Siegel zero part of Proposition 2 implies that for any $\epsilon > 0$, there is a $c(\epsilon, 2)$ such that

$$\beta \leq 1 - c(\epsilon, 2)D^{-\epsilon}$$

where $D = 4N\mathfrak{f}_1$. Thus if we chose $\epsilon = 200$, then $N\mathfrak{f}_1 > \log^{100} \nu$.

Hence (3.15) implies

$$(II) \ll x \log^{-99} \nu$$

For the third sum (III): there is no Siegel zero, so from the explicit formula (2.2) we have for any $\psi(x/N\epsilon, \chi)$ in sum (III), there exist a positive constant c such that

$$\psi(x/N\epsilon, \chi) \ll \frac{x}{N\epsilon} \cdot \log^2 x \cdot \exp\left(-\frac{c \log(x/N\epsilon)}{\log N\epsilon}\right) + \frac{x}{N\epsilon^5} \log^2 x + x^{\frac{1}{4}} N\epsilon^{-\frac{1}{4}} \log(x/N\epsilon)$$

where we have chosen $T = N\epsilon^4$ and used $N\mathfrak{f}_1 \leq 16^2 N\epsilon$. Corresponding to these three terms, we arrive at

$$(III) = \Sigma_1 + \Sigma_2 + \Sigma_3$$

$$\begin{aligned} \Sigma_1 &= x \log^2 x \sum_{\substack{\mu < N\epsilon \leq \nu, \\ \mathfrak{f}_1 \nmid \mu}}^* \frac{1}{N\epsilon} \cdot \exp\left(-c \frac{\log x/N\epsilon}{\log N\epsilon}\right) \\ &\ll x \log^2 x \cdot \exp\left(-c'(\log \log x)^{100}\right) \cdot \sum_{\substack{\mu < N\epsilon \leq \nu, \\ \mathfrak{f}_1 \nmid \mu}}^* \frac{1}{N\epsilon} \\ &\ll x \log^3 x \cdot \exp\left(-c'(\log \log x)^{100}\right) \end{aligned}$$

$$\begin{aligned} \Sigma_2 &= x \log^2 x \sum_{\substack{\mu < N\epsilon \leq \nu, \\ \mathfrak{f}_1 \nmid \mu}}^* N\epsilon^{-5} \ll x \log^2 x \cdot \mu^{-4} \ll x \log^{-200} x \\ \Sigma_3 &\ll x^{\frac{1}{4}} \log x \sum_{\substack{\mu < N\epsilon \leq \nu, \\ \mathfrak{f}_1 \nmid \mu}}^* N\epsilon^{-\frac{1}{4}} \ll x^{\frac{1}{4}} \log x \cdot \nu^{\frac{3}{4}} \ll x^{\frac{1}{2}} \end{aligned}$$

Hence we arrive at

$$(III) = o\left(\frac{x}{\log x}\right)$$

□

Now we prove Lemma 4:

Proof. According to (i),(ii) and Lemma 2, we know that A_ϵ represents those primary class $a \pmod{16\epsilon}$ such that

$$(i') \quad Na \equiv \alpha_k \pmod{16}, \text{ and } \left(\frac{Na}{N\lambda_j}\right) = (-1)^{B_{jk}} \text{ for } 1 \leq j \leq k-1;$$

$$(ii') \quad \left(\frac{2}{a}\right)_4 \left(\frac{a}{\theta_1}\right) = \left(\frac{2}{\epsilon}\right)_4 \left(\frac{\epsilon/\theta_1}{\theta_1}\right) (-1)^{\frac{\Pi_1^k \alpha_j - 1}{8} + \frac{\Pi_1^k \alpha_j^{z_j} - 5}{4}}.$$

From Chinese Remainder Theorem, we have the following identification:

$$\left(\mathbb{Z}[i]/16\epsilon\mathbb{Z}[i]\right)^\times \simeq \left(\mathbb{Z}[i]/16\mathbb{Z}[i]\right)^\times \times \prod_{j=1}^{k-1} \left(\mathbb{Z}[i]/\lambda_j\mathbb{Z}[i]\right)^\times$$

given by $a \mapsto (a_0, a_1, \dots, a_{k-1})$ with a_j the corresponding image of a modulo λ_j and $\lambda_0 := 16$. Then the residue symbol $\left(\frac{\cdot}{\theta_1}\right)$ is trivial on those component $\lambda_j \nmid \theta_1$, and similarly for other residue symbols. Hence the condition $\left(\frac{Na_j}{N\lambda_j}\right) = 1$ selects half of the $\left(\mathbb{Z}[i]/\lambda_j\mathbb{Z}[i]\right)^\times$ -part, since the norm map induces an isomorphism $\left(\mathbb{Z}[i]/\lambda_j\mathbb{Z}[i]\right)^\times \simeq \left(\mathbb{Z}/p_j\mathbb{Z}\right)^\times$ as $p_j = N\lambda_j$ splits completely in $\mathbb{Z}[i]$.

For the part of $\left(\mathbb{Z}[i]/16\mathbb{Z}[i]\right)^\times$, we use the same notation as in Lemma 3. With a_1, \dots, a_{k-1} chosen such that $\left(\frac{Na_j}{N\lambda_j}\right) = 1$, then the remaining conditions of (i'), (ii') are equivalent to

$$\chi_1(g) = i^{\frac{\alpha_k - 1}{4}}, \quad \chi_2(g) = i^\delta \quad (3.16)$$

where $g \in G$ and $i^\delta = \left(\frac{2}{\epsilon}\right)_4 \left(\frac{\epsilon/\theta_1}{\theta_1}\right) \cdot \prod_{\lambda_j \mid \theta_1} \left(\frac{a_j}{\lambda_j}\right) \cdot (-1)^{\frac{\Pi_1^k \alpha_j - 1}{8} + \frac{\Pi_1^k \alpha_j^{z_j} - 5}{4}}$.

Similar as Lemma 3, the existence of $g \in G$ such that (3.16) holds is equivalent to $i^{2 \cdot \frac{\alpha_k - 1}{4}} = i^{2\delta}$. Now we verify this:

$$i^{2\delta} = \left(\frac{2^2}{\eta}\right)_4 = \left(\frac{2}{N\eta}\right) = \left(\frac{2}{\alpha_1 \cdots \alpha_{k-1}}\right) = \left(\frac{2}{\alpha_k}\right)$$

as $\prod_{j=1}^k \alpha_j \equiv 1 \pmod{8}$, while

$$i^{2 \cdot \frac{\alpha_k - 1}{4}} = (-1)^{\frac{\alpha_k - 1}{4}} = \left(\frac{2}{\alpha_k}\right) = i^{2\delta}$$

Therefore the condition (3.16) selects an eighth of G similarly. Consequently

$$\#A_\epsilon = \frac{\phi(16\epsilon)}{2^{k+4}}$$

This completes the proof of the lemma. \square

4 Distribution of Congruent Elliptic Curves

In this section, we will prove the main Theorem and the distribution of those congruent elliptic curves with rank 0 and 2-primary part of Shafarevich-Tate group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$.

According to the strategy explained in the introduction, we first interpret some conceptions related to 8-rank in Gauss genus theory. We refer to §3 of our previous paper [2]. Let $n = p_1 \cdots p_k \equiv 1 \pmod{8}$ in Q_k , denote $\mathcal{A} = \mathcal{A}_n$ the ideal class group of $\mathbb{Q}(\sqrt{-n})$. Then the 2^j -rank $h_{2^j}(n)$ of \mathcal{A} is defined to be $\text{rank}_{\mathbb{F}_2} 2^{j-1} \mathcal{A} / 2^j \mathcal{A}$ with the multiplications in \mathcal{A} written additively, hence $2^j \mathcal{A}$ denotes the subgroup consisting of 2^j -power of elements in \mathcal{A} . Note that from definition we can easily get $h_4(n) = \text{rank}_{\mathbb{F}_2} \mathcal{A}[2] \cap 2\mathcal{A}$, where $\mathcal{A}[2]$

denotes the subgroup consisting of elements with square trivial. Then Gauss genus theory implies that there is a 2 to 1 epimorphism

$$\theta : \{X \in \mathbb{F}_2^{k+1} \mid RX = 0\} \longrightarrow \mathcal{A}[2] \cap 2\mathcal{A} \quad (4.1)$$

with $\theta(X_0)$ trivial, where $X_0 = (1, \dots, 1, 0)^T$ and R is a $k \times (k+1)$ matrix over \mathbb{F}_2 defined by

$$R = (A \mid \mathfrak{b})$$

with $A = (a_{ij})_{k \times k}$ and $\mathfrak{b} = \left(\left[\frac{2}{p_1} \right], \dots, \left[\frac{2}{p_k} \right] \right)^T$, here $a_{ii} = \sum_{l \neq i} a_{il}$, $a_{ij} = \left[\frac{p_j}{p_i} \right]$ with $i \neq j$. Whence we have $h_4(n) = k - \text{rank} R$.

To count the number of certain congruent elliptic curves with $n \in Q_k$ conveniently, we assume that:

The Redie matrix R_n is defined with the p_j arranged increasingly

whence $R = R_n$ and $A = A_n$ is completely determined by n .

4.1 Distribution of $\text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^2$

Theorem 1 of [2] characterizes that $n \in P_k$ if and only if

$$h_4(n) = 1, \quad h_8(n) \equiv \frac{d-5}{4} \pmod{2} \quad (4.2)$$

where $d = \prod_{j=1}^k p_j^{x_j}$ with $X = (x_1, \dots, x_k, x_{k+1})^T \neq X_0$ satisfying $RX = 0$. Moreover two choice of X_1, X_2 doesn't affect $\frac{d-1}{4} \pmod{2}$. In fact, if $h_4(n) = 1$ there are two cases according to $\text{rank} A$ as in the proof of Theorem 1 of [2]:

- (i) If $\text{rank} A_n = k - 1$, let $x = (x_1, \dots, x_k)$ be a non-trivial solution of $Ax = \mathfrak{b}$, then $d = \prod_{j=1}^k p_j^{x_j}$. Then Theorem 3.3(iii),(iv) of Jung-Yue [3] implies that $h_8(n) = 1$ if and only if

$$\left(\frac{2d}{d'} \right)_4 \left(\frac{2d'}{d} \right)_4 = (-1)^{\frac{n-1}{8}}$$

with $n = dd'$. Then by equation (3.1) this is equivalent to

$$\left(\frac{\theta_2}{\theta_1} \right) \left(\frac{2}{n} \right)_4 = (-1)^{\frac{n-1}{8}}$$

where θ_1, θ_2 is the primary integer lying above d, d' with every prime factor in \mathcal{P} .

- (ii) If $\text{rank} A = k - 2$, let $x = (x_1, \dots, x_k) \neq 0, (1, \dots, 1)^T$ such that $Ax = 0$, then $d = \prod_{j=1}^k p_j^{x_j}$ and $d \equiv 5 \pmod{8}$. Then Theorem 3.3(ii) of Jung-Yue [3] implies that $h_8(n) = 1$ if and only if

$$\left(\frac{d}{d'} \right)_4 \left(\frac{d'}{d} \right)_4 = -1$$

where $d'd = n$.

Remark 1. We remark that there is a typo in Theorem 3.3 (iv) of Jung-Yue [3], which is corrected in above (i).

According to this result and our strategy, we use $\mathcal{B} = \mathcal{B}_k$ to denote all the $k \times k$ symmetric- \mathbb{F}_2 matrix with rank $k - 1$ and every row sum 0, similarly use \mathcal{B}' to denote those with rank $k - 2$. Now we divide into two cases according to $B \in \mathcal{B}, \mathcal{B}'$ respectively:

(a): For any $B \in \mathcal{B} = \mathcal{B}_k$ and any $\alpha = (\alpha_1, \dots, \alpha_k)$ with $\alpha_i \in \{1, 5, 9, 13\}$ and $\prod_{j=1}^k \alpha_j \equiv 1 \pmod{8}$: then the contribution of those $n \leq x$ with $A_n = B, p_j \equiv \alpha_j \pmod{16}$ to $\#P_k(x)$ is the number of $C_k(x, \alpha, B)$, where $n = p_1 \cdots p_k$ with p_j arranged in ascending order. Therefore all of these B, α contributes to $\#P_k(x)$ is

$$\Sigma_1 = \sum_{B \in \mathcal{B}} \sum_{\substack{\alpha \\ 8|\alpha_1 \cdots \alpha_k - 1}} \#C_k(x, \alpha, B)$$

By independence of residue symbol Theorem 2, we know this asymptotically equals to

$$2^{-1 - \binom{k}{2} - 3k} \cdot \#C_k(x) \cdot \sum_{B \in \mathcal{B}} \sum_{\substack{\alpha \\ 8|\alpha_1 \cdots \alpha_k - 1}} 1 = 2^{-2-k - \binom{k}{2}} \cdot \#C_k(x) \cdot \#\mathcal{B}$$

So we reduce to compute $\#\mathcal{B}$, which can be accomplished by a result in Brown and many coauthors [14]:

Proposition 3. *Let $\mathcal{B}_{k,r}$ denote all the $k \times k$ symmetric matrix over \mathbb{F}_2 of rank $r \leq k$, then*

$$\#\mathcal{B}_{k,r} = 2^{\binom{r+1}{2}} \cdot u_{r+1} \cdot \prod_{i=0}^{k-r-1} \frac{2^k - 2^i}{2^{k-r} - 2^i}$$

where u_r is defined in Theorem 1.

Note every $B \in \mathcal{B}$ corresponds to a $B' \in \mathcal{B}_{k-1,k-1}$ by summing all rows to last row then delete last row, and similarly for column. Whence we have

$$\#\mathcal{B} = \#\mathcal{B}_k = u_k \cdot 2^{\binom{k}{2}} \quad (4.3)$$

So we arrive at

$$\Sigma_1 \sim 2^{-2-k} \cdot u_k \cdot \#C_k(x)$$

(b): For $B \in \mathcal{B}'$, we denote Σ_B to be the set of $\alpha = (\alpha_1, \dots, \alpha_k)$ with $\alpha_i \in \{1, 5, 9, 13\}$ and $\prod_{j=1}^k \alpha_j \equiv 1 \pmod{8}$ such that

$$\text{rank}_{\mathbb{F}_2}(B|_{\mathfrak{b}_\alpha}) = k - 1$$

where $\mathfrak{b}_\alpha = \left(\left[\frac{2}{\alpha_1} \right], \dots, \left[\frac{2}{\alpha_k} \right] \right)^T$. Then for $B \in \mathcal{B}', \alpha \in \Sigma_B$, the contribution of those $n = p_1 \cdots p_k \leq x$ with $p_1 < \cdots < p_k, A_n = B$ and $p_j \equiv \alpha_j \pmod{16}$ to $\#P_k(x)$ is the number of $C_k(x, \alpha, B)'$, which is defined to be all $n = p_1 \cdots p_k \in C_k(x)$ with p_j arranged increasingly satisfying:

- (1) $p_l \equiv \alpha_l \pmod{16}$;
- (2) $\left(\frac{p_l}{p_j} \right) = (-1)^{B_{lj}}, 1 \leq l < j \leq k$;
- (3) $\left(\frac{d}{d'} \right)_4 \left(\frac{d'}{d} \right)_4 = -1$.

where $dd' = n$ and $d = \prod_{j=1}^k p_j^{x_j}$ with $x \neq 0, (1, \dots, 1)^T$ a vector in \mathbb{F}_2^k such that $Ax = 0$. Note that this case implies that $k \geq 2$.

Before we count all the contribution of $B \in \mathcal{B}'$ and $\alpha \in \Sigma_B$, we first counting the number of \mathcal{B}' and Σ_B respectively.

(b1): As every row sum of $B \in \mathcal{B}'$ is 0, thus adding all rows to the last row then the last row is 0 then delete the last row, similarly for the last column as B is symmetric, thus we get a $B' \in \mathcal{B}_{k-1, k-2}$, thus from Proposition 3 we have

$$\#\mathcal{B}' = 2^{\binom{k-1}{2}} \cdot u_{k-1} \cdot (2^{k-1} - 1) \quad (4.4)$$

(b2): For $B \in \mathcal{B}'$, we want to count the number of those \mathbb{F}_2 -matrix $\mathbf{b} = \mathbf{b}_{k \times 1}$ with column sum 0 such that

$$\text{rank}_{\mathbb{F}_2}(B|\mathbf{b}) = k - 1$$

With similar elementary transforms as B , then $(B|\mathbf{b})$ corresponds to

$$(B'|\mathbf{b}')$$

where \mathbf{b}' obtains from \mathbf{b} with no last term, then the rank of $(B'|\mathbf{b}')$ is $k - 1$ means that \mathbf{b}' is not in the image of B' , thus there are exactly 2^{k-2} many \mathbf{b}' . Whence there are 2^{k-2} such \mathbf{b} . To every \mathbf{b} there are 2^k many $\alpha \in \Sigma_B$: as $b_j = \left\lfloor \frac{2}{\alpha_j} \right\rfloor$ determines $\alpha_j \pmod{8}$, then any α_j has exact two choice. Consequently we have

$$\#\Sigma_B = 2^{2k-2} \quad (4.5)$$

Similarly as Theorem 2, we have the following independence of residue symbol property for $\#C_k(x, \alpha, B)'$:

$$\#C_k(x, \alpha, B)' \sim 2^{-1-3k-\binom{k}{2}} \#C_k(x) \quad (4.6)$$

Thus the contribution of all $B \in \mathcal{B}'$ and $\alpha \in \Sigma_B$ is

$$\Sigma_2 = \sum_{B \in \mathcal{B}'} \sum_{\alpha \in \Sigma_B} \#C_k(x, \alpha, B)' \sim 2^{-1-3k-\binom{k}{2}} \sum_{B \in \mathcal{B}'} \sum_{\alpha \in \Sigma_B} \#C_k(x)$$

Then from (4.4) and (4.5), Σ_2 asymptotically equals to

$$2^{-1-3k-\binom{k}{2}} \#\mathcal{B}' \cdot \#\Sigma_B \cdot \#C_k(x) = 2^{-2-2k}(2^{k-1} - 1)u_{k-1} \#C_k(x)$$

From (i),(ii) we know $\#P_k(x) = \Sigma_1 + \Sigma_2$, therefore

$$\begin{aligned} \#P_k(x) &\sim 2^{-2-k} \left(u_k + (2^{-1} - 2^{-k})u_{k-1} \right) \#C_k(x) \\ \lim_{x \rightarrow \infty} \frac{\#P_k(x)}{\#Q_k(x)} &= \frac{1}{2} \left(u_k + (2^{-1} - 2^{-k})u_{k-1} \right) \end{aligned}$$

where we have used the fact that

$$\#Q_k(x) \sim 2^{-1-k} \cdot \#C_k(x)$$

which can be easily verified by independence of residue symbol property of Rhoades [4]. Whence we finish the proof of Theorem 1.

4.2 Distribution of $\text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^4$

In this subsection, we mainly discuss the distribution of congruent elliptic curves $E^{(n)}$ with $\text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^4$, see the following theorem:

Theorem 3. *Let $\tilde{Q}_k(x)$ be the set of positive squarefree integers $n \leq x$ with exact k prime factors and all prime factors of n are congruent to 1 (mod 8), and $\tilde{P}_k(x)$ consists of those $n \in \tilde{Q}_k(x)$ satisfying*

$$\text{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0, \quad \text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^4$$

Then for any $k \geq 2$ we have

$$\lim_{x \rightarrow \infty} \frac{\#\tilde{P}_k(x)}{\#\tilde{Q}_k(x)} \geq 2^{k-4} \cdot \sum_{\substack{j_1+j_2=k \\ j_1, j_2 \geq 1}} u_{j_1} u_{j_2} \cdot \binom{k}{j_1} \cdot 2^{-j_1 j_2}$$

where u_j is defined in Theorem 1.

Given $k, k' \geq 1$, Theorem 1.2 and Remark 4 of our previous paper [2] shows that $n \in \tilde{P}_{k+k'}$ if $n = dd' \in \tilde{Q}_{k+k'}$ with $\omega(d) = k, \omega(d') = k'$ such that

- (i) $\left(\frac{p}{p'}\right) = 1$ with p, p' any prime divisor of d, d' respectively;
- (ii) $h_4(d) = h_4(d') = 1$;
- (iii) $\left(\frac{2}{d}\right)_4 = (-1)^{\frac{d-9}{8}}, \left(\frac{2}{d'}\right)_4 = (-1)^{\frac{d'-9}{8}}$ and $\left(\frac{d}{d'}\right)_4 = \left(\frac{d'}{d}\right)_4 = 1$.

In fact Theorem 4.1 and Corollary 1 of that paper [2] give more general conditions make n lie in $\tilde{P}_{k+k'}$, but for easy of notation we just limited to (i)-(iii).

To count the contribution of those n satisfying (i)-(iii), we need some notations. Let $k, k' \geq 1$ and $\sigma = \{\sigma_1, \dots, \sigma_k\}$ be an ascending subsequence of $1, \dots, k+k'$ with exact k elements, and $\sigma' = \{\sigma'_1, \dots, \sigma'_{k'}\}$ be the remained increasing subsequence of $1, \dots, k+k'$ by deleting those elements of σ . Moreover we let \mathcal{S} to denote all these σ , then $\#\mathcal{S} = \binom{k+k'}{k}$. We also let \mathcal{R} to denote the set of $\alpha = (\alpha_1, \dots, \alpha_{k+k'})$ with every $\alpha_j \in \{1, 9\}$, then $\#\mathcal{R} = 2^{2(k+k')}$. For $\alpha \in \mathcal{R}$, $B \in \mathcal{B}_k, B' \in \mathcal{B}_{k'}$ and $\sigma \in \mathcal{S}$, we denote $C_{k,k'}(x, \alpha, B, B', \sigma)$ to be those $n = p_1 \cdots p_{k+k'} \in \tilde{Q}_{k+k'}(x)$ with p_j arranged increasingly such that

- (1) $p_j \equiv \alpha_j \pmod{16}$ for $1 \leq j \leq k+k'$;
- (2) $A_d = B, A_{d'} = B'$ with $d = \prod_{j=1}^k p_{\sigma_j}, d' = \prod_{j=1}^{k'} p_{\sigma'_j}$;
- (3) $\left(\frac{p}{p'}\right) = 1$ with p, p' any prime divisor of d, d' respectively;
- (4) $\left(\frac{2}{d}\right)_4 = (-1)^{\frac{\delta-9}{8}}, \left(\frac{2}{d'}\right)_4 = (-1)^{\frac{\delta'-9}{8}}$ with $\delta = \prod_{j=1}^k \alpha_{\sigma_j}, \delta' = \prod_{j=1}^{k'} \alpha_{\sigma'_j}$;
- (5) $\left(\frac{d}{d'}\right)_4 = \left(\frac{d'}{d}\right)_4 = 1$.

Then similar as independence of residue symbol Theorem 2, we have

$$\#C_{k,k'}(x, \alpha, B, B', \sigma) \sim \frac{1}{2^{4+3(k+k')+\binom{k+k'}{2}}} \cdot \#C_{k+k'}(x)$$

Moreover from (i)-(iii) we know $C_{k,k'}(x, \alpha, B, B', \sigma)$ is contained in $\tilde{P}_{k+k'}(x)$. Therefore all the contribution of those $C_{k,k'}(x, \alpha, B, B', \sigma)$ with $\alpha \in \mathcal{R}$, $B \in \mathcal{B}_k, B' \in \mathcal{B}_{k'}, \sigma \in \mathcal{S}$ to $\tilde{P}_{k+k'}(x)$ is

$$\begin{aligned}
& \sum_{\alpha \in \mathcal{R}} \sum_{B \in \mathcal{B}_k} \sum_{B' \in \mathcal{B}_{k'}} \sum_{\sigma \in \mathcal{S}} \#C_{k,k'}(x, \alpha, B, B', \sigma) \\
& \sim \frac{\#\mathcal{R} \cdot \#\mathcal{B}_k \cdot \#\mathcal{B}_{k'} \cdot \#\mathcal{S}}{2^{4+3(k+k')+\binom{k+k'}{2}}} \cdot \#C_{k+k'}(x) \\
& = \frac{u_k u_{k'} \cdot \binom{k+k'}{k} \cdot 2^{2(k+k')+\binom{k}{2}+\binom{k'}{2}}}{2^{4+3(k+k')+\binom{k+k'}{2}}} \cdot \#C_{k+k'}(x) \\
& = \frac{u_k u_{k'} \cdot \binom{k+k'}{k}}{2^{4+k+k'+kk'}} \cdot \#C_{k+k'}(x)
\end{aligned}$$

where we have used (4.3). Note from independence of residue symbol property of Rhoades [4], we have

$$\#\tilde{Q}_k(x) \sim 2^{-2k} \cdot \#C_k(x)$$

Consequently we have

$$\lim_{x \rightarrow \infty} \frac{\#\tilde{P}_k(x)}{\#\tilde{Q}_k(x)} \geq 2^{k-4} \cdot \sum_{\substack{j_1+j_2=k \\ j_1, j_2 \geq 1}} u_{j_1} u_{j_2} \cdot \binom{k}{j_1} \cdot 2^{-j_1 j_2}$$

Acknowledgements

I am greatly indebted to Professor Ye Tian, my supervisor, for many instructions and suggestions! I would like to thank Lvhao Yan for carefully reading the manuscript and giving valuable comments.

References

- [1] V. Vatsal, ‘Rank-one twists of a certain elliptic curve,’ *Mathematische Annalen*, vol. 311, no. 4(1998)pp. 791–794.
- [2] Z. Wang, ‘Congruent elliptic curves with non-trivial Shafarevich-Tate group,’ *preprint*.
- [3] H. Jung and Q. Yue, ‘8-ranks of class groups of imaginary quadratic number fields and their densities,’ *J. Korean Math. Soc.* vol. 48, no. 6(2011)pp. 1249–1268.
- [4] R. Rhoades, ‘2-Selmer groups and the Birch–Swinnerton-Dyer Conjecture for the congruent number curves,’ *J. Number Theory*, vol. 129, no. 6(2009)pp. 1379–1391.
- [5] J. Cremona and R. Odoni, ‘Some density results for negative Pell equations: an application of graph theory,’ *J. London Math. Soc. (2)*, vol. 39, no. 1(1989) pp. 16–28.
- [6] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, second edition(1990, Springer-Verlag)pp. xiv+389.
- [7] H. Iwaniec and E. Kowalski, *Analytic number theory*, AMS Colloquium Publications, vol. 53(2004, AMS Providence)pp. xii+615.

- [8] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Mathematics, vol. 77(1981, Springer-Verlag)pp. xii+239.
- [9] E. Fogels, ‘Über die Ausnahmenullstelle der Heckschen L-Funktionen,’ *Acta Arith.*, vol. 8, no. 3(1963)pp. 307–309.
- [10] E. Fogels, ‘On the zeros of L-functions,’ *Acta Arith.*, vol. 11, no. 1(1962)pp. 67–96.
- [11] E. Fogels, ‘Corrigendum to the paper ”On the zeros of L-functions” (Acta Arith. 11(1965)pp. 67-96),’ *Acta Arith.*, vol. 14, no. 4(1968) pp. 435.
- [12] J. Hoffstein and D. Ramakrishnan, ‘Siegel zeros and cusp forms,’ *Internat. Math. Res. Notices*, vol. 1995, no. 6(1995) pp. 279–308.
- [13] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics, vol. 110, second edition(1994, Springer-Verlag)pp. xiv+357.
- [14] M. Brown, N. Calkin, K. James, A. King, S. Lockard and R. Rhoades, ‘Trivial selmer groups and even partitions of a graph,’ *Integers*, vol. 6, no. A33 (2006)pp.17.

Zhangjie Wang,
 Yau Mathematical Sciences Center,
 Tsinghua University, Beijing 100084, China.
 zjwang@math.tsinghua.edu.cn